



# Interfaces logiques

ONTAP 9

NetApp

February 06, 2026

This PDF was generated from [https://docs.netapp.com/fr-fr/ontap/networking/configure\\_lifs\\_cluster\\_administrators\\_only\\_overview.html](https://docs.netapp.com/fr-fr/ontap/networking/configure_lifs_cluster_administrators_only_overview.html) on February 06, 2026.  
Always check [docs.netapp.com](https://docs.netapp.com) for the latest.

# Sommaire

Interfaces logiques . . . . .	1
Présentation de la LIF . . . . .	1
En savoir plus sur la configuration LIF d'un cluster ONTAP . . . . .	1
En savoir plus sur la compatibilité des LIF ONTAP avec les types de ports . . . . .	3
Politiques de service LIF et rôles pris en charge pour votre version ONTAP . . . . .	4
Découvrez les LIF ONTAP et les règles de service . . . . .	5
Gestion des LIF . . . . .	11
Configurer des politiques de service LIF pour un cluster ONTAP . . . . .	11
Création des LIF ONTAP . . . . .	17
Modifiez les LIFs ONTAP . . . . .	24
Migrez les LIF ONTAP . . . . .	26
Restaure une LIF sur son port d'attache après un basculement de nœud ONTAP ou une migration de port . . . . .	29
Restaurer une LIF ONTAP mal configurée . . . . .	30
Supprimez les LIFs ONTAP . . . . .	31
Configuration des LIF ONTAP Virtual IP (VIP) . . . . .	31
Configuration du protocole BGP (Border Gateway Protocol) . . . . .	32
Créer une LIF de données VIP (Virtual IP) . . . . .	37
Commandes de gestion du protocole BGP . . . . .	38

# Interfaces logiques

## Présentation de la LIF

### En savoir plus sur la configuration LIF d'un cluster ONTAP

Une LIF (Logical interface) représente un point d'accès réseau à un nœud du cluster. Vous pouvez configurer les LIF sur les ports sur lesquels le cluster envoie et reçoit des communications sur le réseau.

Un administrateur de cluster peut créer, afficher, modifier, migrer, restaurer, Ou supprimez les LIFs. Un administrateur SVM ne peut afficher que les LIFs associées à la SVM.

Une LIF est une adresse IP ou un WWPN qui présente des caractéristiques associées, telles qu'une politique de service, un port d'accueil, un nœud de rattachement, une liste de ports à basculer et une politique de pare-feu. Vous pouvez configurer les LIF sur les ports sur lesquels le cluster envoie et reçoit des communications sur le réseau.



Depuis ONTAP 9.10.1, les politiques de pare-feu sont obsolètes et intégralement remplacées par les politiques de service de LIF. Pour plus d'informations, voir "[Configuration des politiques de pare-feu pour les LIF](#)".

Les LIFs peuvent être hébergées sur les ports suivants :

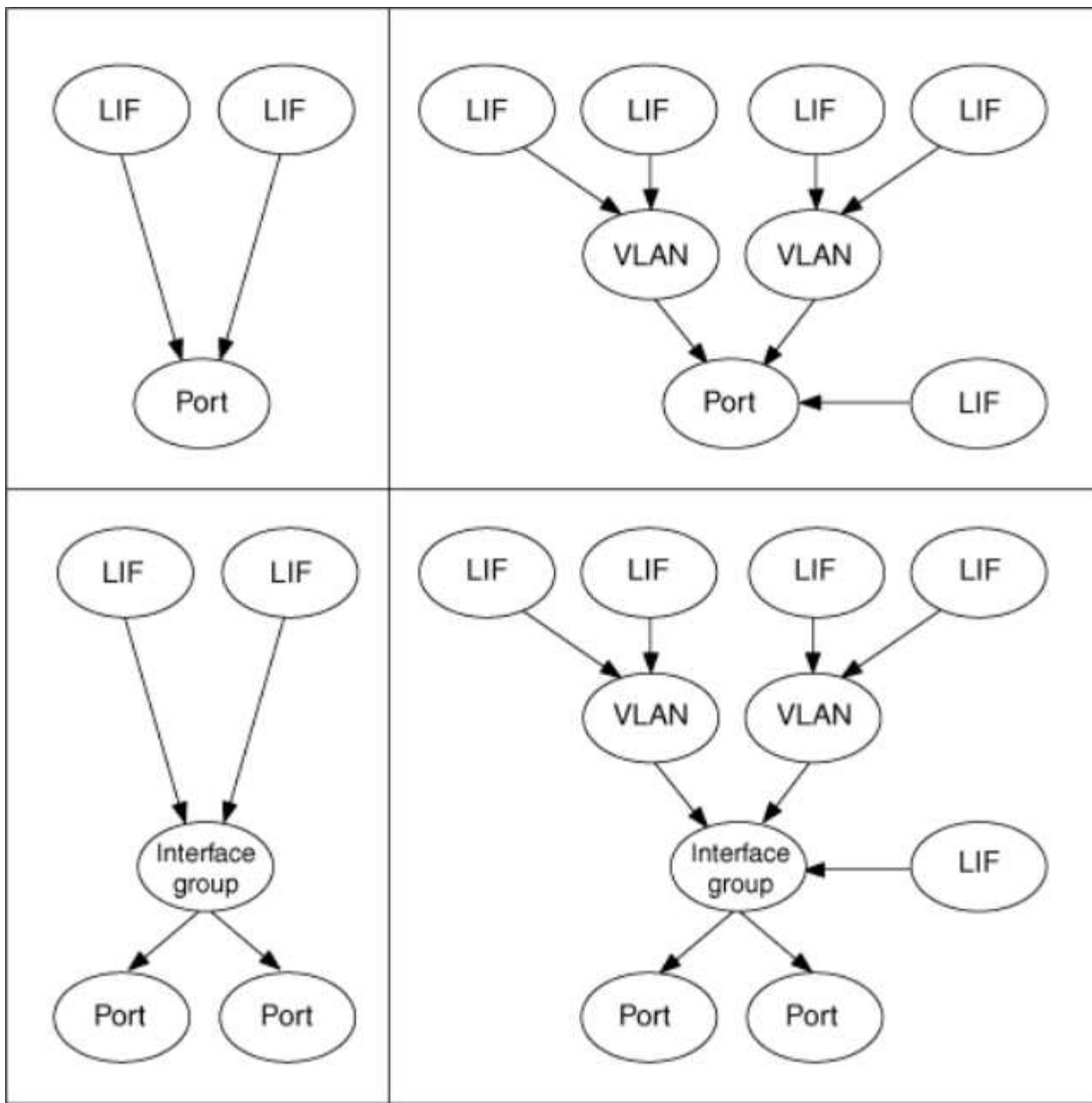
- Ports physiques ne faisant pas partie de groupes d'interfaces
- Groupes d'interface
- VLAN
- Ports physiques ou groupes d'interfaces qui hébergent des VLAN
- Ports VIP (Virtual IP)

Depuis ONTAP 9.5, les LIFs VIP sont prises en charge et hébergées sur des ports VIP.

Lors de la configuration des protocoles SAN tels que FC sur une LIF, ils seront associés à un WWPN.

### ["Administration SAN"](#)

La figure suivante illustre la hiérarchie de ports dans un système ONTAP :



### Basculement et rétablissement de LIF

Un basculement de LIF se produit lorsqu'une LIF se déplace de son nœud ou port de rattachement vers le nœud ou le port HA Partner. Un basculement de LIF peut être déclenché automatiquement par ONTAP ou manuellement par un administrateur du cluster pour certains événements, tels qu'un lien Ethernet physique en panne ou un nœud qui dévie du quorum de la base de données répliquée (RDB). Lorsqu'un basculement de LIF se produit, ONTAP continue son fonctionnement normal sur le nœud partenaire jusqu'à ce que la raison du basculement soit résolue. Lorsque le nœud ou le port de rattachement retrouve sa santé, la LIF est reconvertie du partenaire HA en nœud ou port de rattachement. Ce retour s'appelle un retour.

Pour le basculement et le rétablissement LIF, les ports de chaque nœud doivent appartenir au même broadcast domain. Pour vérifier que les ports appropriés de chaque nœud appartiennent au même broadcast domain, consultez les documents suivants :

- ONTAP 9.8 et versions ultérieures : ["Réparation de l'accessibilité de l'orifice"](#)

- ONTAP 9.7 et versions antérieures : ["Ajouter ou supprimer des ports d'un broadcast domain"](#)

Pour les LIF avec basculement LIF activé (automatiquement ou manuellement), les points suivants s'appliquent :

- Pour les LIF utilisant une policy de service de données, vous pouvez vérifier les restrictions de failover-policy :
  - ONTAP 9.6 et versions ultérieures : ["LIF et politiques de services dans ONTAP 9.6 et versions ultérieures"](#)
  - ONTAP 9.5 et versions antérieures : ["Rôles LIF dans ONTAP 9.5 et versions antérieures"](#)
- La restauration automatique des LIF se produit lorsque la restauration automatique est définie sur `true` Et lorsque le port de attache de la LIF est sain et peut héberger la LIF.
- En cas de basculement de nœud planifié ou non planifié, la LIF sur le nœud repris bascule vers le partenaire haute disponibilité. Le port sur lequel la LIF tombe en panne est déterminé par vif Manager.
- Une fois le basculement terminé, le LIF fonctionne normalement.
- Lorsqu'un rétablissement est initié, la LIF retourne à son nœud et port de rattachement, si la restauration automatique est définie sur `true`.
- Lorsqu'une liaison ethernet est indisponible sur un port hébergeant une ou plusieurs LIF, vif Manager migre les LIFs du port DOWN vers un autre port du même broadcast domain. Le nouveau port peut se trouver sur le même nœud ou sur son partenaire HA. Une fois la liaison restaurée et si la restauration automatique est définie sur `true`, Le vif Manager restaure les LIF sur leur nœud de rattachement et leur port de rattachement.
- Lorsqu'un nœud quitte le quorum RDB (Replicated database), il migre les LIF du nœud de quorum vers son partenaire haute disponibilité. Une fois que le nœud revient au quorum et que la restauration automatique est définie sur `true`, Le vif Manager restaure les LIF sur leur nœud de rattachement et leur port de rattachement.

## En savoir plus sur la compatibilité des LIF ONTAP avec les types de ports

Les LIF peuvent présenter des caractéristiques différentes pour prendre en charge différents types de ports.

 Lorsque les LIF intercluster et de gestion sont configurées dans le même sous-réseau, le trafic de gestion peut être bloqué par un pare-feu externe et les connexions AutoSupport et NTP peuvent tomber en panne. Vous pouvez restaurer le système en exécutant la commande `network interface modify -vserver vserver name -lif intercluster LIF -status -admin up|down` pour basculer le LIF intercluster. Cependant, vous devez définir la LIF intercluster et la LIF de gestion dans différents sous-réseaux pour éviter ce problème.

LIF	Description
-----	-------------

LIF de données	<p>LIF associée à un SVM (Storage Virtual machine) et servant à la communication avec les clients.</p> <p>Vous pouvez avoir plusieurs LIFs data sur un port. Ces interfaces peuvent migrer ou basculer sur l'ensemble du cluster. Vous pouvez modifier une LIF de données afin de servir de LIF de gestion SVM en modifiant sa politique de pare-feu en gestion.</p> <p>Les sessions établies aux serveurs NIS, LDAP, Active Directory, WINS, et DNS utilisent les LIFs data.</p>
LIF Cluster	<p>Une LIF utilisée pour acheminer le trafic intracluster entre les nœuds d'un cluster. Les LIFs cluster doivent toujours être créées sur les ports de type cluster.</p> <p>Les LIFs de cluster peuvent basculer entre les ports de cluster sur le même nœud, mais elles ne peuvent pas être migrées ou basculer vers un nœud distant. Lorsqu'un nouveau nœud rejoint un cluster, les adresses IP sont générées automatiquement. Toutefois, si vous souhaitez attribuer manuellement des adresses IP aux LIF de cluster, vous devez vous assurer que les nouvelles adresses IP se trouvent dans la même plage de sous-réseau que les LIF de cluster existantes.</p>
LIF Cluster-management	<p>LIF qui offre une interface de gestion unique pour l'ensemble du cluster.</p> <p>Une LIF de cluster management peut basculer vers n'importe quel nœud du cluster. Il ne peut pas basculer vers le cluster ou les ports intercluster</p>
FRV InterCluster	<p>LIF utilisée pour la communication, la sauvegarde et la réplication entre clusters. Vous devez créer une LIF intercluster sur chaque node du cluster avant qu'une relation de peering de cluster ne puisse être établie.</p> <p>Ces LIFs peuvent uniquement basculer sur les ports du même nœud. Ils ne peuvent pas être migrés ni basculés vers un autre nœud du cluster.</p>
FRV de gestion des nœuds	<p>Une LIF qui fournit une adresse IP dédiée pour gérer un nœud particulier dans un cluster. Les LIFs de node-management sont créées au moment de la création ou de l'arrivée du cluster. Ces LIFs sont utilisées pour la maintenance du système, par exemple lorsqu'un nœud devient inaccessible depuis le cluster.</p>
LIF VIP	<p>Une LIF VIP est toute LIF de données créée sur un port VIP. Pour en savoir plus, voir "<a href="#">Configuration des LIF IP virtuelles (VIP)</a>".</p>

#### Informations associées

- ["modification de l'interface réseau"](#)

## Politiques de service LIF et rôles pris en charge pour votre version ONTAP

Au fil du temps, la façon dont ONTAP gère le type de trafic pris en charge sur les LIF a changé.

- ONTAP 9.5 et les versions antérieures utilisent des rôles LIF et des services de pare-feu.
- Les versions ONTAP 9.6 et ultérieures utilisent les stratégies de service LIF :
  - La version ONTAP 9.5 a introduit les stratégies de service LIF.

- ONTAP 9.6 a remplacé les rôles LIF par des stratégies de service LIF.
- ONTAP 9.10.1 a remplacé les services de pare-feu par des politiques de service LIF.

La méthode que vous configurez dépend de la version de ONTAP que vous utilisez.

Pour en savoir plus sur :

- Politiques de pare-feu, voir "[Commande : firewall-policy-show](#)".
- Rôles LIF, voir "[Rôles LIF \(ONTAP 9.5 et versions antérieures\)](#)".
- Politiques de service LIF, voir "[LIF et règles de service \(ONTAP 9.6 et versions ultérieures\)](#)".

## Découvrez les LIF ONTAP et les règles de service

Vous pouvez attribuer des politiques de service (au lieu de rôles LIF ou de politiques de pare-feu) aux LIF qui déterminent le type de trafic pris en charge pour les LIF. Les stratégies de service définissent une collection de services réseau prise en charge par une LIF. ONTAP fournit un ensemble de règles de service intégrées qui peuvent être associées à une LIF.



La méthode de gestion du trafic réseau est différente dans ONTAP 9.7 et les versions antérieures. Si vous devez gérer le trafic sur un réseau exécutant ONTAP 9.7 et les versions antérieures, reportez-vous à la section "[Rôles LIF \(ONTAP 9.5 et versions antérieures\)](#)".



Les protocoles FCP et NVMe/FCP ne nécessitent actuellement pas de service-policy.

Vous pouvez afficher les stratégies de service et leurs détails à l'aide de la commande suivante :

```
network interface service-policy show
```

Pour en savoir plus, `network interface service-policy show` consultez le "[Référence de commande ONTAP](#)".

Les fonctionnalités qui ne sont pas liées à un service spécifique utiliseront un comportement défini par le système pour sélectionner les LIFs pour les connexions sortantes.



Les applications qui se trouvent sur une LIF avec une politique de service vide peuvent se comporter de manière inattendue.

## Règles de service pour les SVM système

Le SVM d'administration et tout SVM système contiennent des politiques de service qui peuvent être utilisées pour les LIF au sein de ce SVM, y compris les LIFs de type management et intercluster. Ces règles sont automatiquement créées par le système lorsqu'un IPspace est créé.

Le tableau suivant répertorie les règles intégrées pour les LIF dans les SVM système à partir de ONTAP 9.12.1. Pour les autres versions, afficher les politiques de service et leurs détails à l'aide de la commande suivante :

```
network interface service-policy show
```

Politique	Services inclus	Rôle équivalent	Description
valeur-par-défaut intercluster	intercluster-core, management-https	intercluster	Utilisé par les LIFs transportant le trafic intercluster. Attention : le service intercluster est disponible depuis le ONTAP 9.5 avec le nom net-intercluster service policy.
annonce-route-par-défaut	gestion-bgp	-	Utilisé par les LIFs transportant des connexions homologues BGP Remarque : disponible auprès de ONTAP 9.5 avec le nom net-route-announce service policy.
gestion par défaut	management-core, management-https, management-http, management-ssh, management-autosupport, management-ems, management-dns-client, management-ad-client, management-ldap-client, management-nis-client, management-ntp-client, transfert-journalisation-gestion	nœuds de gestion et de gestion de cluster	Utilisez cette politique de gestion étendue du système pour créer des LIFs de gestion du type node-and-cluster détenues par un SVM système. Ces LIF peuvent être utilisées pour les connexions sortantes vers des serveurs DNS, AD, LDAP ou NIS, ainsi que pour prendre en charge des connexions supplémentaires pour prendre en charge les applications s'exécutant pour le compte de l'ensemble du système. À partir de ONTAP 9.12.1, vous pouvez utiliser le management-log-forwarding service pour contrôler les LIFs utilisées pour transférer les journaux d'audit à un serveur syslog distant.

Le tableau suivant liste les services que les LIFs peuvent utiliser sur un SVM système depuis ONTAP 9.11.1 :

Service	Limites du basculement	Description
intercluster-core	home-node-seulement	Services intercluster de base
cœur de gestion	-	Services de gestion centrale
management-ssh	-	Services d'accès à la gestion SSH
gestion-http	-	Services de gestion de l'accès HTTP
gestion-https	-	Services pour l'accès à la gestion HTTPS
gestion-autosupport	-	Services liés à l'imputation de charges utiles AutoSupport

gestion-bgp	port d'origine uniquement	Services liés aux interactions BGP par les pairs
backup-ndmp-control	-	Services pour les commandes de sauvegarde NDMP
gestion-ems	-	Services d'accès à la messagerie de gestion
client-ntp-management	-	Introduit dans ONTAP 9.10.1. Services pour l'accès client NTP.
serveur-ntp-management	-	Introduit dans ONTAP 9.10.1. Services pour l'accès à la gestion de serveurs NTP
management-portmap	-	Services de gestion de portmap
serveur-rsh de gestion	-	Services de gestion de serveur rsh
serveur-gestion-snmp	-	Services de gestion de serveur SNMP
serveur-telnet-gestion	-	Services de gestion de serveur telnet
transfert de journaux de gestion	-	Introduit dans ONTAP 9.12.1. Services de transfert de journaux d'audit

### Règles de service pour les SVM de données

Tous les SVM de données contiennent des règles de service qui peuvent être utilisées par les LIF de ce SVM.

Le tableau ci-dessous répertorie les règles intégrées pour les LIF dans des SVM de données commençant par ONTAP 9.11.1. Pour les autres versions, afficher les politiques de service et leurs détails à l'aide de la commande suivante :

```
network interface service-policy show
```

Politique	Services inclus	Protocole de données équivalent	Description
gestion par défaut	data-core, management-https, management-http, management-ssh, management-dns-client, management-ad-client, management-ldap-client, management-nis-client	Aucune	Utiliser cette politique de gestion « SVM-scoped » pour créer des LIFs de management du SVM détenues par un SVM de données. Ces LIF peuvent fournir un accès SSH ou HTTPS aux administrateurs du SVM. Lorsque nécessaire, ces LIF peuvent être utilisées pour des connexions sortantes vers des serveurs DNS externes, AD, LDAP ou NIS.

blocs de données par défaut	coeur de données, iscsi	iscsi	Utilisée par les LIF transportant un trafic de données SAN orienté bloc. Depuis ONTAP 9.10.1, la règle « default-data-blocks » est obsolète. Utilisez plutôt la stratégie de service « default-data-iscsi ».
fichiers-données-par-défaut	data-core, data-fpolicy-client, data-dns-serveur, data-FlexCache, data-cifs, data-nfs, management-dns-client, management-ad-client, management-ldap-client, management-nis-client	nfs, cifs, fcache	Utilisez la stratégie par défaut-data-Files pour créer des LIF NAS qui prennent en charge des protocoles de données basés sur des fichiers. Parfois, il n'y a qu'une seule LIF présente au SVM, donc cette politique permet à la LIF d'être utilisée pour les connexions sortantes vers un serveur DNS externe, AD, LDAP ou NIS. Si vous préférez que ces connexions utilisent uniquement des LIF de gestion, vous pouvez supprimer ces services à partir de cette règle.
iscsi-données-par-défaut	coeur de données, iscsi	iscsi	Utilisé par les LIF transportant le trafic de données iSCSI.
données-défaut-nvme-tcp	coeur de données, nvme-tcp	nvme-tcp	Utilisé par les LIF transportant du trafic de données NVMe/TCP.

Le tableau ci-dessous répertorie les services pouvant être utilisés sur un SVM de données ainsi que les restrictions imposées par chaque service à la politique de basculement d'une LIF à partir de la ONTAP 9.11.1 :

Service	Restrictions de basculement	Description
management-ssh	-	Services d'accès à la gestion SSH
gestion-http	-	Introduit dans ONTAP 9.10.1 Services de gestion de l'accès HTTP
gestion-https	-	Services pour l'accès à la gestion HTTPS
management-portmap	-	Services d'accès à la gestion de portmap
serveur-gestion-snmp	-	Introduit dans ONTAP 9.10.1 Services pour l'accès à la gestion de serveur SNMP
coeur des données	-	Services de données centrales
nfs-données	-	Service de données NFS
cifs-données	-	Service de données CIFS

flexcache	-	Service de données FlexCache
iscsi données	Port d'attache uniquement pour l'AFF/FAS ; partenaire sfo uniquement pour ASA	Service de données iSCSI
backup-ndmp-control	-	Introduit dans ONTAP 9.10.1 Backup NDMP contrôle le service de données
serveur-données-dns	-	Introduit dans ONTAP 9.10.1 Service de données du serveur DNS
client-données fpolicy	-	Service de données de stratégie de filtrage de fichiers
tcp-nvme-données	port d'origine uniquement	Introduit dans ONTAP 9.10.1 Service de données TCP NVMe
serveur data s3	-	Service de données des serveurs simple Storage Service (S3)

Vous devez savoir comment les règles de service sont attribuées aux LIF dans les SVM de données :

- Lorsqu'un SVM de données est créé avec une liste de services de données, les règles de service « fichiers de données par défaut » et « blocs de données par défaut » intégrées à ce SVM sont créées à l'aide des services spécifiés.
- Si un SVM de données est créé sans spécifier une liste de services de données, les règles de service « fichiers de données par défaut » et « blocs de données par défaut » intégrées à ce SVM sont créées à l'aide d'une liste de services de données par défaut.

La liste des services de données par défaut comprend les services iSCSI, NFS, NVMe, SMB et FlexCache.

- Lorsqu'une LIF est créée avec une liste de protocoles de données, une politique de service équivalente aux protocoles de données spécifiés est assignée à la LIF.
- Si aucune stratégie de service équivalente n'existe, une stratégie de service personnalisée est créée.
- Lorsqu'une LIF est créée sans une policy de service ou une liste de protocoles de données, la politique de service default-data-Files est assignée à la LIF par défaut.

## Service Data-core

Le service « Data-core » permet à des composants qui utilisaient auparavant les LIF avec le rôle de données de fonctionner comme prévu sur les clusters mis à niveau pour gérer les LIF à l'aide de politiques de service plutôt que de rôles LIF (qui sont obsolètes dans ONTAP 9.6).

La spécification data-core en tant que service n'ouvre aucun port du pare-feu, mais le service doit être inclus dans toute politique de service d'un SVM de données. Par exemple, la règle de service Default-data-Files contient les services suivants par défaut :

- cœur des données

- nfs-données
- cifs-données
- flexcache

Le service « data-core » doit être inclus dans la règle afin de garantir que toutes les applications utilisant la LIF comme prévu, mais que les trois autres services peuvent être supprimés, si nécessaire.

### Service LIF côté client

Depuis ONTAP 9.10.1, ONTAP fournit des services LIF côté client pour de nombreuses applications. Ces services permettent de contrôler les LIFs utilisées pour les connexions sortantes pour le compte de chaque application.

Les nouveaux services suivants permettent aux administrateurs de contrôler la liste des LIF utilisées comme adresses source pour certaines applications.

Service	Restrictions des SVM	Description
client-annonce-gestion	-	Depuis ONTAP 9.11.1, ONTAP fournit un service client Active Directory pour les connexions sortantes vers un serveur AD externe.
client-dns-gestion	-	À partir de ONTAP 9.11.1, ONTAP fournit un service client DNS pour les connexions sortantes vers un serveur DNS externe.
gestion-ldap-client	-	Depuis ONTAP 9.11.1, ONTAP fournit un service client LDAP pour les connexions sortantes vers un serveur LDAP externe.
gestion-nis-client	-	À partir de ONTAP 9.11.1, ONTAP fournit un service client NIS pour les connexions sortantes à un serveur NIS externe.
client-ntp-management	système uniquement	Depuis ONTAP 9.10.1, ONTAP fournit un service client NTP pour les connexions sortantes vers un serveur NTP externe.
client-données fpolicy	données uniquement	Depuis ONTAP 9.8, ONTAP fournit un service client pour les connexions FPolicy de sortie.

Chacun des services est automatiquement inclus dans certaines règles de service intégrées, mais les administrateurs peuvent les supprimer des règles intégrées ou les ajouter à des règles personnalisées afin de contrôler les LIF utilisées pour les connexions sortantes pour le compte de chaque application.

### Informations associées

- ["Interface réseau service-policy show"](#)

# Gestion des LIF

## Configurer des politiques de service LIF pour un cluster ONTAP

Vous pouvez configurer les stratégies de service LIF afin d'identifier un seul service ou une liste de services qui utiliseront une LIF.

### Création d'une policy de service pour les LIFs

Vous pouvez créer une policy de service pour les LIF. Vous pouvez affecter une stratégie de service à une ou plusieurs LIF, permettant ainsi au LIF de transporter du trafic pour un seul service ou une liste de services.

Vous avez besoin de privilèges avancés pour exécuter la commande `network interface service-policy create`.

### Description de la tâche

Les services et les règles de service intégrés sont disponibles pour la gestion du trafic de données et de gestion sur les SVM de données et de système. La plupart des cas d'utilisation sont satisfaits à l'aide d'une règle de service intégrée plutôt que de créer une règle de service personnalisée.

Vous pouvez modifier ces règles de service intégrées, si nécessaire.

### Étapes

1. Afficher les services disponibles dans le cluster :

```
network interface service show
```

Les services représentent les applications auxquelles un LIF accède, ainsi que les applications servies par le cluster. Chaque service inclut zéro ou plus de ports TCP et UDP sur lesquels l'application écoute.

Les services de gestion et de données supplémentaires suivants sont disponibles :

```
cluster1::> network interface service show

Service                                Protocol:Ports
-----
cluster-core                           -
data-cifs                               -
data-core                               -
data-flexcache                         -
data-iscsi                             -
data-nfs                               -
intercluster-core                      tcp:11104-11105
management-autosupport                 -
management-bgp                          tcp:179
management-core                         -
management-https                       tcp:443
management-ssh                          tcp:22
12 entries were displayed.
```

2. Afficher les politiques de service qui existent dans le cluster :

```

cluster1::> network interface service-policy show

Vserver      Policy                      Service: Allowed Addresses
-----  -----
-----  -----
cluster1
    default-intercluster      intercluster-core: 0.0.0.0/0
                                management-https: 0.0.0.0/0

    default-management        management-core: 0.0.0.0/0
                                management-autosupport: 0.0.0.0/0
                                management-ssh: 0.0.0.0/0
                                management-https: 0.0.0.0/0

    default-route-announce   management-bgp: 0.0.0.0/0

Cluster
    default-cluster          cluster-core: 0.0.0.0/0

vs0
    default-data-blocks      data-core: 0.0.0.0/0
                                data-iscsi: 0.0.0.0/0

    default-data-files       data-core: 0.0.0.0/0
                                data-nfs: 0.0.0.0/0
                                data-cifs: 0.0.0.0/0
                                data-flexcache: 0.0.0.0/0

    default-management       data-core: 0.0.0.0/0
                                management-ssh: 0.0.0.0/0
                                management-https: 0.0.0.0/0

7 entries were displayed.

```

### 3. Création d'une règle de services :

```

cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver <svm_name>
-policies <service_policy_name> -services <service_name> -allowed
-addresses <IP_address/mask,...>

```

- « nom\_service » indique une liste de services à inclure dans la stratégie.
- "IP\_address/mask" spécifie la liste des masques de sous-réseau pour les adresses autorisées à accéder aux services dans la stratégie de service. Par défaut, tous les services spécifiés sont ajoutés avec une liste d'adresses par défaut autorisée de 0.0.0.0/0, ce qui permet le trafic de tous les sous-réseaux. Lorsqu'une liste d'adresses autorisées par défaut est fournie, les LIF utilisant la règle sont configurées pour bloquer toutes les demandes avec une adresse source qui ne correspond à aucun des masques spécifiés.

L'exemple suivant montre comment créer une stratégie de service de données, *svm1\_Data\_policy*, pour une SVM qui inclut *NFS* et *SMB* services :

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver svm1
-policies svm1_data_policy -services data-nfs,data-cifs,data-core
```

L'exemple suivant montre comment créer une politique de service intercluster :

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver cluster1
-policies intercluster1 -services intercluster-core
```

4. Vérifiez que la stratégie de service est créée.

```
cluster1::> network interface service-policy show
```

Le résultat suivant indique les règles de service disponibles :

```

cluster1::> network interface service-policy show

Vserver      Policy                                Service: Allowed Addresses
-----  -----
-----  -----
cluster1
    default-intercluster      intercluster-core: 0.0.0.0/0
                                management-https: 0.0.0.0/0

    intercluster1            intercluster-core: 0.0.0.0/0

    default-management       management-core: 0.0.0.0/0
                                management-autosupport: 0.0.0.0/0
                                management-ssh: 0.0.0.0/0
                                management-https: 0.0.0.0/0

    default-route-announce  management-bgp: 0.0.0.0/0

Cluster
    default-cluster          cluster-core: 0.0.0.0/0

vs0
    default-data-blocks      data-core: 0.0.0.0/0
                                data-iscsi: 0.0.0.0/0

    default-data-files       data-core: 0.0.0.0/0
                                data-nfs: 0.0.0.0/0
                                data-cifs: 0.0.0.0/0
                                data-flexcache: 0.0.0.0/0

    default-management       data-core: 0.0.0.0/0
                                management-ssh: 0.0.0.0/0
                                management-https: 0.0.0.0/0

    svm1_data_policy         data-core: 0.0.0.0/0
                                data-nfs: 0.0.0.0/0
                                data-cifs: 0.0.0.0/0

9 entries were displayed.

```

#### Une fois que vous avez terminé

Assigner la policy de service à une LIF soit au moment de la création, soit en modifiant une LIF existante.

## Assigner une policy de service à une LIF

Vous pouvez affecter une policy de service à une LIF au moment de la création de cette LIF ou en modifiant la LIF. Une policy de service définit la liste de services qui peuvent être utilisés avec la LIF.

### Description de la tâche

Vous pouvez attribuer des règles de service pour les LIF dans les SVM admin et data.

### Étape

Selon l'heure à laquelle vous souhaitez affecter la policy de service à une LIF, effectuez l'une des actions suivantes :

Si vous êtes...	Affecter la stratégie de service...
Création d'une LIF	Interface réseau create -vserver svm_name -lif <lif_name> -home-node <nom_node> -home-port <nom_port> {(-adresse <adresse_IP> -masque de réseau <adresse_IP>) -subnet-name <nom_sous-réseau>} -service-policy <nom_service>
Modification d'une LIF	interface réseau modify -vserver <svm_name> -lif <lif_name> -service-policy <service_name>

Lorsque vous spécifiez une policy de services pour une LIF, il n'est pas nécessaire de spécifier le protocole de données et le rôle de cette dernière. La création des LIF en spécifiant le rôle et les protocoles de données est également pris en charge.



Une politique de service peut uniquement être utilisée par les LIFs dans le même SVM que vous avez spécifié lors de la création de la policy de service.

### Exemples

L'exemple suivant montre comment modifier la policy de service d'une LIF pour utiliser la policy de service de gestion par défaut :

```
cluster1::> network interface modify -vserver cluster1 -lif lif1 -service -policy default-management
```

### Commandes permettant de gérer les règles de service LIF

Utilisez le `network interface service-policy` Commandes permettant de gérer les règles de service LIF.

Pour en savoir plus, `network interface service-policy` consultez le "[Référence de commande ONTAP](#)".

### Avant de commencer

La modification de la politique de service d'une LIF dans une relation SnapMirror active interrompt la planification de la réplication. Si vous convertissez une LIF de intercluster en non-intercluster (ou inversement), ces modifications ne sont pas répliquées sur le cluster peering. Pour mettre à jour le Peer Cluster après avoir modifié la politique de service LIF, effectuez d'abord la procédure `snapmirror abort` ensuite [resynchroniser la relation de réplication](#).

Les fonctions que vous recherchez...	Utilisez cette commande...
Création d'une stratégie de service (privileges avancés requis)	network interface service-policy create
Ajouter une entrée de service supplémentaire à une stratégie de service existante (privileges avancés requis)	network interface service-policy add-service
Cloner une stratégie de service existante (privileges avancés requis)	network interface service-policy clone
Modification d'une entrée de service dans une stratégie de service existante (privileges avancés requis)	network interface service-policy modify-service
Suppression d'une entrée de service d'une stratégie de service existante (privileges avancés requis)	network interface service-policy remove-service
Renommer une stratégie de service existante (privileges avancés requis)	network interface service-policy rename
Suppression d'une stratégie de service existante (privileges avancés requis)	network interface service-policy delete
Restaurer une stratégie de service intégrée à son état d'origine (privileges avancés requis)	network interface service-policy restore-defaults
Afficher les stratégies de service existantes	network interface service-policy show

#### Informations associées

- ["présentation du service d'interface réseau"](#)
- ["stratégie de service de l'interface réseau"](#)
- ["annulation de snapmirror"](#)

## Création des LIF ONTAP

Un SVM fournit des données aux clients via une ou plusieurs interfaces logiques réseau (LIF). Vous devez créer les LIFs sur les ports que vous souhaitez utiliser pour accéder aux données. Une LIF (interface réseau) est une adresse IP associée à un port physique ou logique. En cas de panne d'un composant, une LIF peut basculer vers un autre port physique ou la migrer vers un autre port, ce qui continue à communiquer avec le réseau.

#### Et des meilleures pratiques

Les ports de commutateur connectés à ONTAP doivent être configurés en tant que ports de périphérie « spanning Tree » afin de réduire les retards lors de la migration des LIF.

## Avant de commencer

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Le port réseau physique ou logique sous-jacent doit avoir été configuré pour que le statut administratif soit activé.
- Si vous prévoyez d'utiliser un nom de sous-réseau pour allouer la valeur de l'adresse IP et du masque de réseau à une LIF, le sous-réseau doit déjà exister.

Les sous-réseaux contiennent un pool d'adresses IP qui appartiennent au même sous-réseau de couche 3. Ils sont créés à l'aide de System Manager ou de `network subnet create` commande.

Pour en savoir plus, `network subnet create` consultez le "[Référence de commande ONTAP](#)".

- Le mécanisme de spécification du type de trafic traité par une LIF a changé. Pour ONTAP 9.5 et versions antérieures, la LIF utilisait des rôles pour spécifier le type de trafic qu'elle entraînerait. Depuis ONTAP 9.6, les LIF utilisent des politiques de service pour spécifier le type de trafic qu'elles seraient à traiter.

## Description de la tâche

- Vous ne pouvez pas attribuer des protocoles NAS et SAN à la même LIF.

Les protocoles pris en charge sont SMB, NFS, FlexCache, iSCSI et FC ; ISCSI et FC ne peuvent pas être associés à d'autres protocoles. Les protocoles NAS et SAN Ethernet peuvent toutefois être présents sur le même port physique.

- Vous ne devez pas configurer les LIF qui transportent le trafic SMB afin de revenir automatiquement à leurs nœuds de départ. Cette recommandation est obligatoire si le serveur SMB doit héberger une solution pour la continuité de l'activité avec Hyper-V ou SQL Server over SMB.

- Vous pouvez créer des LIF IPv4 et IPv6 sur le même port réseau.
- Tous les services de mappage de noms et de résolution de noms d'hôte utilisés par un SVM, tel que DNS, NIS, LDAP, et Active Directory, Doit être accessible à partir d'au moins une LIF gérant le trafic de données du SVM.
- Une LIF gérant le trafic intracluster entre des nœuds ne doit pas se trouver sur le même sous-réseau que le trafic de gestion d'une LIF ou encore le trafic de données géré par une LIF.
- La création d'une LIF ne disposant pas de cible de basculement valide entraîne un message d'avertissement.
- Si vous disposez d'un grand nombre de LIF dans le cluster, vous pouvez vérifier la capacité LIF prise en charge sur le cluster :
  - System Manager : depuis ONTAP 9.12.0, consultez le débit de la grille de l'interface réseau.
  - Interface de ligne de commandes : utilisez le `network interface capacity show` Et la capacité LIF prise en charge sur chaque nœud à l'aide de `network interface capacity details show` commande (au niveau de privilège avancé).

Pour en savoir plus sur `network interface capacity show` et `network interface capacity details show` dans le "[Référence de commande ONTAP](#)".

- Depuis ONTAP 9.7, si d'autres LIF existent déjà pour le SVM dans le même sous-réseau, il n'est pas nécessaire de spécifier le home port de la LIF. ONTAP choisit automatiquement un port aléatoire sur le nœud de rattachement spécifié dans le même domaine de diffusion que les autres LIFs déjà configurées dans le même sous-réseau.

Le protocole FC-NVMe est pris en charge à partir de la version ONTAP 9.4. Si vous créez une LIF FC-

NVMe, notez les éléments suivants :

- Le protocole NVMe doit être pris en charge par l'adaptateur FC sur lequel la LIF est créée.
- FC-NVMe est le seul protocole de données sur les LIF de données.
- Un trafic de gestion des LIF doit être configuré pour chaque SVM (Storage Virtual machine) prenant en charge les protocoles SAN.
- Les LIFs et namespaces NVMe doivent être hébergés sur le même nœud.
- Un maximum de deux LIF NVMe traitant le trafic de données peut être configuré par SVM, par nœud.
- Lorsque vous créez une interface réseau avec un sous-réseau, ONTAP sélectionne automatiquement une adresse IP disponible à partir du sous-réseau sélectionné et l'attribue à l'interface réseau. Vous pouvez modifier le sous-réseau s'il y a plusieurs sous-réseaux, mais vous ne pouvez pas modifier l'adresse IP.
- Lorsque vous créez (ajoutez) un SVM, pour une interface réseau, vous ne pouvez pas spécifier une adresse IP comprise dans la plage d'un sous-réseau existant. Vous recevrez une erreur de conflit de sous-réseau. Ce problème survient sur d'autres flux de production d'une interface réseau, comme la création ou la modification des interfaces réseau inter-cluster dans les paramètres des SVM ou les paramètres du cluster.
- Depuis la version ONTAP 9.10.1, les `network interface` commandes CLI incluent un `-rdma-protocols` paramètre pour les configurations NFS sur RDMA. La création d'interfaces réseau pour les configurations NFS sur RDMA est prise en charge dans System Manager à partir de ONTAP 9.12.1. Pour plus d'informations, voir [Configuration DES LIF pour NFS sur RDMA](#).
- Depuis la version ONTAP 9.11.1, le basculement automatique des LIF iSCSI est disponible sur les plateformes ASA (All-Flash SAN Array).

Le basculement de LIF iSCSI est automatiquement activé (la règle de basculement est définie sur `sfo-partner-only` la valeur de restauration automatique est définie sur `true`) Sur les LIF iSCSI nouvellement créées si aucune LIF iSCSI n'existe dans le SVM spécifié ou si toutes les LIFs iSCSI existantes du SVM spécifié sont déjà activées avec le basculement LIF iSCSI.

Si après une mise à niveau vers ONTAP 9.11.1 ou version ultérieure, vous disposez de LIF iSCSI existantes dans un SVM qui n'ont pas été activées avec la fonctionnalité de basculement LIF iSCSI et que vous créez de nouvelles LIF iSCSI dans le même SVM, les nouvelles LIF iSCSI supposent la même politique de basculement (`disabled`) Des LIFs iSCSI existantes du SVM.

#### ["Basculement de LIF iSCSI pour les plateformes ASA"](#)

Depuis ONTAP 9.7, ONTAP choisit automatiquement le port de base d'une LIF, tant qu'au moins une LIF existe déjà dans le même sous-réseau dans cet IPspace. ONTAP choisit un port home-port dans le même domaine de diffusion que d'autres LIFs de ce sous-réseau. Vous pouvez toujours spécifier un port home port, mais ce n'est plus nécessaire (sauf si aucune LIF n'existe encore dans ce sous-réseau dans l'IPspace spécifié).

Depuis ONTAP 9.12.0, la procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

## System Manager

### Utilisez System Manager pour ajouter une interface réseau

#### Étapes

1. Sélectionnez **réseau > Présentation > interfaces réseau**.
2. Sélectionnez **+ Add**.
3. Sélectionnez l'un des rôles d'interface suivants :
  - a. Les données
  - b. Intercluster
  - c. Gestion SVM
4. Sélectionnez le protocole :
  - a. SMB/CIFS ET NFS
  - b. ISCSI
  - c. FC
  - d. NVMe/FC
  - e. NVMe/TCP
5. Nommez la LIF ou acceptez le nom généré par vos sélections précédentes.
6. Acceptez le nœud de départ ou utilisez le menu déroulant pour en sélectionner un.
7. Si au moins un sous-réseau est configuré dans l'IPspace du SVM sélectionné, la liste déroulante sous-réseau est affichée.
  - a. Si vous sélectionnez un sous-réseau, choisissez-le dans la liste déroulante.
  - b. Si vous continuez sans sous-réseau, la liste déroulante broadcast domain s'affiche :
    - i. Spécifiez l'adresse IP. Si l'adresse IP est utilisée, un message d'avertissement s'affiche.
    - ii. Spécifiez un masque de sous-réseau.
8. Sélectionnez le port d'accueil dans le domaine de diffusion, soit automatiquement (recommandé), soit en sélectionnant un dans le menu déroulant. Le contrôle du port Home s'affiche en fonction du domaine de diffusion ou de la sélection du sous-réseau.
9. Enregistrez l'interface réseau.

#### CLI

### Utilisez l'interface de ligne de commande pour créer une LIF

#### Étapes

1. Déterminez les ports de broadcast domain que vous souhaitez utiliser pour le LIF.

```
network port broadcast-domain show -ipspace ipspace1
```

IPspace	Broadcast		Update	
Name	Domain name	MTU	Port List	Status Details
ipspace1	default	1500	node1:e0d node1:e0e node2:e0d node2:e0e	complete complete complete complete

Pour en savoir plus, `network port broadcast-domain show` consultez le "[Référence de commande ONTAP](#)".

2. Vérifiez que le sous-réseau que vous souhaitez utiliser pour les LIF contient suffisamment d'adresses IP inutilisées.

`network subnet show -ipspace ipspace1`

Pour en savoir plus, `network subnet show` consultez le "[Référence de commande ONTAP](#)".

3. Créez une ou plusieurs LIF sur les ports que vous souhaitez utiliser pour accéder aux données.

 NetApp recommande la création d'objets de sous-réseau pour toutes les LIFs sur les SVM de données. Cela est particulièrement important dans les configurations MetroCluster, où l'objet de sous-réseau permet à ONTAP de déterminer les cibles de basculement sur le cluster de destination, car chaque objet de sous-réseau possède un broadcast associé. Pour obtenir des instructions, reportez-vous à "[Créez un sous-réseau](#)" la .

```
network interface create -vserver _SVM_name_ -lif _lif_name_
-service-policy _service_policy_name_ -home-node _node_name_ -home
-port port_name {-address _IP_address_ - netmask _Netmask_value_ |
-subnet-name _subnet_name_} -firewall- policy _policy_ -auto-revert
{true|false}
```

- ° `-home-node` Est le nœud vers lequel la LIF renvoie lorsque `network interface revert` La commande est exécutée sur le LIF.

Vous pouvez également indiquer si la LIF doit revenir automatiquement au nœud home et au port home-port avec l'option `-auto-revert`.

Pour en savoir plus, `network interface revert` consultez le "[Référence de commande ONTAP](#)".

- ° `-home-port` Est le port physique ou logique vers lequel la LIF renvoie lorsque `network interface revert` La commande est exécutée sur le LIF.
- ° Vous pouvez spécifier une adresse IP avec le `-address` et `-netmask` ou vous activez l'allocation à partir d'un sous-réseau avec `-subnet_name` option.

- Lors de l'utilisation d'un sous-réseau pour fournir l'adresse IP et le masque de réseau, si le sous-réseau a été défini avec une passerelle, une route par défaut vers cette passerelle est ajoutée automatiquement au SVM lorsqu'une LIF est créée à l'aide de ce sous-réseau.
- Si vous attribuez des adresses IP manuellement (sans utiliser de sous-réseau), vous devrez peut-être configurer une route par défaut vers une passerelle si des clients ou des contrôleurs de domaine se trouvent sur un autre sous-réseau IP. Pour en savoir plus, `network route create` consultez le "[Référence de commande ONTAP](#)".
- `-auto-revert` Vous permet de spécifier si une LIF de données est automatiquement rétablie sur le nœud de rattachement en cas de démarrage, de modifications du statut de la base de données de gestion ou lors de la connexion réseau. Le paramètre par défaut est `false`, mais vous pouvez le définir sur `true` selon les stratégies de gestion de réseau de votre environnement.
- `-service-policy` Depuis ONTAP 9.5, vous pouvez attribuer une policy de service pour la LIF avec le `-service-policy` option.  
Lorsqu'une politique de services est spécifiée pour une LIF, cette règle est utilisée pour construire un rôle par défaut, une politique de basculement et une liste de protocoles de données pour la LIF. Dans ONTAP 9.5, les stratégies de service sont prises en charge uniquement pour les services de pairs intercluster et BGP. Dans ONTAP 9.6, vous pouvez créer des stratégies de service pour plusieurs services de données et de gestion.
- `-data-protocol` Permet de créer une LIF qui prend en charge les protocoles FCP ou NVMe/FC. Cette option n'est pas requise lors de la création d'une LIF IP.

4. **Facultatif** : attribuez une adresse IPv6 dans l'option `-address` :

- Utilisez le `network ndp prefix show` Commande permettant d'afficher la liste des préfixes de RA apprises sur diverses interfaces.

Le `network ndp prefix show` la commande est disponible au niveau de privilège avancé.

Pour en savoir plus, `network ndp prefix show` consultez le "[Référence de commande ONTAP](#)".

- Utiliser le format `prefix:::id` Pour construire l'adresse IPv6 manuellement.

`prefix` est le préfixe utilisé sur les différentes interfaces.

Pour calculer le `id`, choisissez un nombre hexadécimal 64 bits aléatoire.

5. Vérifier que la configuration de l'interface LIF est correcte.

```
network interface show -vserver vs1
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
vs1	lif1	up/up	10.0.0.128/24	node1	e0d	
true						

Pour en savoir plus, `network interface show` consultez le "[Référence de commande ONTAP](#)".

#### 6. Vérifiez que la configuration du groupe de basculement est la plus appropriée.

```
network interface show -failover -vserver vs1
```

Vserver	Logical interface	Home Node:Port	Failover Policy	Failover Group
vs1	lif1	node1:e0d	system-defined	ipspace1

Failover Targets: node1:e0d, node1:e0e, node2:e0d, node2:e0e

#### 7. Vérifiez que l'adresse IP configurée est accessible :

Pour vérifier...	Utiliser...
Adresse IPv4	ping réseau
Adresse IPv6	réseau ping6

#### Exemples

La commande suivante crée une LIF et spécifie les valeurs d'adresse IP et de masque réseau à l'aide de `-address` et `-netmask` paramètres :

```
network interface create -vserver vs1.example.com -lif data1if1
-service-policy default-data-files -home-node node-4 -home-port e1c
-address 192.0.2.145 -netmask 255.255.255.0 -auto-revert true
```

La commande suivante crée une LIF et attribue des valeurs d'adresse IP et de masque réseau à partir du sous-réseau spécifié (nommé `client1_sub`) :

```
network interface create -vserver vs3.example.com -lif data1if3
-service-policy default-data-files -home-node node-3 -home-port e1c
-subnet-name client1_sub - auto-revert true
```

La commande suivante crée une LIF NVMe/FC et spécifie le `nvme-fc` protocole de données :

```
network interface create -vserver vs1.example.com -lif datalif1 -data
-protocol nvme-fc -home-node node-4 -home-port 1c -address 192.0.2.145
-netmask 255.255.255.0 -auto-revert true
```

## Modifiez les LIFs ONTAP

Vous pouvez modifier une LIF en modifiant les attributs, tels que le nœud de rattachement ou le nœud actuel, l'état administratif, l'adresse IP, le masque de réseau, la règle de basculement, la politique de pare-feu et la politique de service. Vous pouvez également modifier la famille d'adresses d'une LIF d'IPv4 à IPv6.

### Description de la tâche

- Lorsque vous modifiez le statut administratif d'une LIF en cas de panne, tout verrouillage NFSv4 en attente est conservé jusqu'à ce que le statut administratif de la LIF soit renvoyé à une date supérieure.

Pour éviter les conflits de verrouillage pouvant survenir lorsque d'autres LIFs tentent d'accéder aux fichiers verrouillés, vous devez déplacer les clients NFSv4 vers une autre LIF avant de définir le statut administratif sur `down`.

- Vous ne pouvez pas modifier les protocoles de données utilisés par une LIF FC. Toutefois, vous pouvez modifier les services affectés à une politique de service ou modifier la politique de service attribuée à une LIF IP.

Pour modifier les protocoles de données utilisés par une LIF FC, il faut supprimer cette LIF, puis la recréer. Pour modifier la stratégie de service à une LIF IP, une brève interruption se produit lors des mises à jour.

- Vous ne pouvez pas modifier le nœud de rattachement ou le nœud actuel d'un LIF de management scoped `node-scoped`.
- Lors de l'utilisation d'un sous-réseau pour modifier l'adresse IP et la valeur du masque réseau d'une LIF, une adresse IP est allouée à partir du sous-réseau spécifié ; si l'adresse IP précédente de la LIF provient d'un autre sous-réseau, l'adresse IP est renvoyée à ce sous-réseau.
- Pour modifier la famille d'adresses d'une LIF d'IPv4 vers IPv6, vous devez utiliser la notation des deux-points pour l'adresse IPv6 et ajouter une nouvelle valeur pour le `-netmask-length` paramètre.
- Vous ne pouvez pas modifier les adresses IPv6 lien-local configurées automatiquement.
- La modification d'une LIF entraînant l'absence de cible de basculement valide entraîne un message d'avertissement.

Si une LIF ne disposant pas de tentatives de basculement cible valides, une panne peut se produire.

- Depuis ONTAP 9.5, vous pouvez modifier la politique de service associée à une LIF.

Dans ONTAP 9.5, les stratégies de service sont prises en charge uniquement pour les services de pairs intercluster et BGP. Dans ONTAP 9.6, vous pouvez créer des stratégies de service pour plusieurs services de données et de gestion.

- Depuis la version ONTAP 9.11.1, le basculement automatique des LIF iSCSI est disponible sur les

plateformes ASA (All-Flash SAN Array).

Pour les LIF iSCSI préexistantes, c'est-à-dire les LIF créées avant la mise à niveau vers la version 9.11.1 ou ultérieure, vous pouvez modifier la règle de basculement sur incident en "[Activer le basculement automatique de LIF iSCSI](#)".

- ONTAP utilise le protocole NTP (Network Time Protocol) pour synchroniser l'heure sur le cluster. Après avoir modifié les adresses IP LIF, vous devrez peut-être mettre à jour la configuration NTP pour éviter les échecs de synchronisation. Pour plus d'informations, reportez-vous à la "[Base de connaissances NetApp : Échec de la synchronisation NTP après un changement d'adresse IP LIF](#)".

La procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

## System Manager

À partir de ONTAP 9.12.0, vous pouvez utiliser System Manager pour modifier une interface réseau

### Étapes

1. Sélectionnez **réseau > Présentation > interfaces réseau**.
2. Sélectionnez  > **Modifier** en regard de l'interface réseau que vous souhaitez modifier.
3. Modifiez un ou plusieurs paramètres de l'interface réseau. Pour plus de détails, voir "[Créer une LIF](#)".
4. Enregistrez les modifications.

## CLI

Utilisez l'interface de ligne de commande pour modifier une LIF

### Étapes

1. Modifier les attributs d'une LIF à l'aide de `network interface modify` commande.

L'exemple suivant montre comment modifier l'adresse IP et le masque de réseau de LIF `datalif2` en utilisant une adresse IP et la valeur du masque de réseau de `subnet client1_sub` :

```
network interface modify -vserver vs1 -lif datalif2 -subnet-name
client1_sub
```

L'exemple suivant montre comment modifier la politique de service d'une LIF.

```
network interface modify -vserver siteA -lif node1_inter1 -service
-policy example
```

Pour en savoir plus, `network interface modify` consultez le "[Référence de commande ONTAP](#)".

2. Vérifiez que les adresses IP sont accessibles.

Si vous utilisez...	Puis utilisez...
Adresses IPv4	<code>network ping</code>
Adresses IPv6	<code>network ping6</code>

Pour en savoir plus, `network ping` consultez le "[Référence de commande ONTAP](#)".

## Migrez les LIF ONTAP

Vous pouvez avoir à migrer une LIF vers un autre port du même nœud ou d'un autre

nœud du cluster, si le port est défectueux ou nécessite une maintenance. La migration d'une LIF est similaire au basculement de LIF, mais la migration de LIF est une opération manuelle, tandis que le basculement de LIF est la migration automatique d'une LIF en réponse à une défaillance de liaison sur le port réseau actuel du LIF.

#### Avant de commencer

- Un failover group doit avoir été configuré pour les LIFs.
- Le nœud et les ports de destination doivent être opérationnels et doivent pouvoir accéder au même réseau que le port source.

#### Description de la tâche

- Les LIF BGP résident sur le port de rattachement et ne peuvent pas être migrées vers un autre nœud ou port.
- Vous devez migrer les LIFs hébergées sur les ports appartenant à une carte réseau vers d'autres ports du cluster, avant de retirer la carte réseau du nœud.
- Vous devez exécuter la commande pour migrer une LIF de cluster à partir du nœud sur lequel la LIF de cluster est hébergée.
- Un LIF node-scoped, tel qu'une LIF node-scoped management, cluster LIF, intercluster LIF, ne peut pas être migré vers un nœud distant.
- Lorsqu'une LIF NFSv4 est migrée entre les nœuds, un délai de 45 secondes peut atteindre les résultats avant que la LIF ne soit disponible sur un nouveau port.

Pour contourner ce problème, utilisez NFSv4.1 en cas de retard.

- Vous pouvez migrer des LIF iSCSI sur des plateformes ASA exécutant ONTAP 9.11.1 ou une version ultérieure.

La migration des LIF iSCSI est limitée aux ports du nœud de rattachement ou du partenaire de haute disponibilité.

- Si votre plateforme n'est pas une baie SAN 100 % Flash (ASA) exécutant ONTAP version 9.11.1 ou ultérieure, vous ne pouvez pas migrer les LIF iSCSI d'un nœud vers un autre.

Pour contourner cette restriction, vous devez créer une LIF iSCSI sur le nœud de destination. En savoir plus sur "[Création des LIFs iSCSI](#)".

- Si vous souhaitez migrer une LIF (interface réseau) pour NFS sur RDMA, vous devez vous assurer que le port de destination est compatible RoCE. Vous devez exécuter ONTAP 9.10.1 ou version ultérieure pour migrer une LIF avec l'interface de ligne de commandes ou ONTAP 9.12.1 pour effectuer la migration à l'aide de System Manager. Dans System Manager, une fois que vous avez sélectionné votre port de destination compatible RoCE, vous devez cocher la case en regard de **utiliser les ports RoCE** pour terminer la migration. En savoir plus sur "[Configuration des LIFs pour NFS sur RDMA](#)".
- Les opérations de déchargement des copies VMware VAAI échouent lors de la migration du LIF source ou de destination. En savoir plus sur la copie hors chargement :
  - "[Les environnements NFS](#)"
  - "[Environnements SAN](#)"

La procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

## System Manager

### Utilisez System Manager pour migrer une interface réseau

#### Étapes

1. Sélectionnez **réseau > Présentation > interfaces réseau**.
2. Sélectionnez  > **migrer** en regard de l'interface réseau à modifier.



Pour une LIF iSCSI, dans la boîte de dialogue **Migrate interface**, sélectionnez le nœud de destination et le port du partenaire HA.

Si vous souhaitez migrer définitivement la LIF iSCSI, cochez la case. La LIF iSCSI doit être hors ligne avant d'être définitivement migrée. De plus, une fois la migration permanente d'une LIF iSCSI, celle-ci ne peut pas être annulée. Il n'y a pas d'option de restauration.

3. Cliquez sur **migrer**.
4. Enregistrez les modifications.

#### CLI

### Utilisez l'interface de ligne de commande pour migrer une LIF

#### Étape

Selon que vous souhaitez migrer une LIF ou toutes les LIF, effectuez l'action appropriée :

Pour migrer...	Saisissez la commande suivante...
Une LIF spécifique	network interface migrate
Toutes les LIF de gestion des données et du cluster sur un nœud	network interface migrate-all
Toutes les LIFs hors d'un port	network interface migrate-all -node <node> -port <port>

L'exemple suivant montre comment migrer une LIF nommée `datalif1` Sur le SVM `vs0` vers le port `e0d` marche `node0b`:

```
network interface migrate -vserver vs0 -lif datalif1 -dest-node node0b  
-dest-port e0d
```

L'exemple suivant montre comment migrer toutes les LIFs de données et cluster-management depuis le nœud actuel (local) :

```
network interface migrate-all -node local
```

## Informations associées

- ["migration des interfaces réseau"](#)

## Restaure une LIF sur son port d'attache après un basculement de nœud ONTAP ou une migration de port

Vous pouvez restaurer une LIF vers son port de base après qu'elle échoue ou qu'elle est migrée vers un autre port manuellement ou automatiquement. Si le port de home d'une LIF particulière n'est pas disponible, la LIF reste sur son port actuel et n'est pas rétablie.

### Description de la tâche

- Si vous rétablir d'un point de vue administratif l'état du port de base d'une LIF avant de configurer l'option de restauration automatique, la LIF n'est pas renvoyée au port de base.
- La LIF ne revient pas automatiquement, sauf si la valeur de l'option « auto-revert » est définie sur vrai.
- Vous devez vous assurer que l'option de restauration automatique est activée pour que les LIF puissent revenir à leurs ports de base.

La procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

### System Manager

#### Utilisez System Manager pour rétablir une interface réseau à son port d'accueil

##### Étapes

1. Sélectionnez **réseau > Présentation > interfaces réseau**.
2. Sélectionnez  > **Revert** en regard de l'interface réseau que vous souhaitez modifier.
3. Sélectionnez **Revert** pour rétablir une interface réseau à son port d'origine.

### CLI

#### Utilisez l'interface de ligne de commande pour rétablir une LIF à son port d'accueil

##### Étape

Restaurez une LIF manuellement ou automatiquement sur son port de base :

Si vous souhaitez restaurer une LIF vers son port de base...	Entrez ensuite la commande suivante...
Manuellement	<code>network interface revert -vserver vserver_name -lif lif_name</code>
Automatiquement	<code>network interface modify -vserver vserver_name -lif lif_name -auto-revert true</code>

Pour en savoir plus, `network interface` consultez le "["Référence de commande ONTAP"](#)".

## Restaurer une LIF ONTAP mal configurée

Un cluster ne peut pas être créé lorsque le réseau de cluster est câblé à un commutateur, mais tous les ports configurés dans le Cluster IPspace peuvent atteindre les autres ports configurés dans le Cluster IPspace.

### Description de la tâche

Dans un cluster commuté, si une interface réseau de cluster (LIF) est configurée sur le port inapproprié ou si un port de cluster est câblé dans le mauvais réseau, la commande `cluster create` peut échouer avec l'erreur suivante :

```
Not all local cluster ports have reachability to one another.  
Use the "network port reachability show -detail" command for more details.
```

Pour en savoir plus, `cluster create` consultez le ["Référence de commande ONTAP"](#).

Les résultats de la `network port show` commande peuvent afficher que plusieurs ports sont ajoutés au Cluster IPspace car ils sont connectés à un port configuré avec une LIF de cluster. Cependant, les résultats de la `network port reachability show -detail` la commande révèle quels ports n'ont pas de connectivité entre eux.

Pour en savoir plus, `network port show` consultez le ["Référence de commande ONTAP"](#).

Pour restaurer une LIF de cluster configurée sur un port qui n'est pas accessible aux autres ports configurés avec des LIFs de cluster, effectuez les opérations suivantes :

### Étapes

1. Réinitialiser le home port de la LIF de cluster sur le port correct :

```
network port modify -home-port
```

Pour en savoir plus, `network port modify` consultez le ["Référence de commande ONTAP"](#).

2. Retirer les ports qui ne disposent pas de LIFs de cluster configurées sur eux du cluster broadcast domain :

```
network port broadcast-domain remove-ports
```

Pour en savoir plus, `network port broadcast-domain remove-ports` consultez le ["Référence de commande ONTAP"](#).

3. Création du cluster :

```
cluster create
```

### Résultat

Une fois le cluster créé, le système détecte la configuration correcte et place les ports dans les domaines de diffusion appropriés.

#### Informations associées

- ["affichage de l'accessibilité des ports réseau"](#)

## Supprimez les LIFs ONTAP

Vous pouvez supprimer une interface réseau (LIF) qui n'est plus requise.

#### Avant de commencer

Les LIFs à supprimer ne doivent pas être en cours d'utilisation.

#### Étapes

1. Marquez les LIFs que vous souhaitez supprimer comme administrativement arrêtées à l'aide de la commande suivante :

```
network interface modify -vserver vserver_name -lif lif_name -status  
-admin down
```

2. Utilisez le `network interface delete` Commande de suppression d'une ou de l'ensemble des LIFs :

Si vous souhaitez supprimer...	Entrez la commande ...
Une LIF spécifique	<code>network interface delete -vserver vserver_name -lif lif_name</code>
Toutes les LIF	<code>network interface delete -vserver vserver_name -lif *</code>

Pour en savoir plus, `network interface delete` consultez le ["Référence de commande ONTAP"](#).

La commande suivante supprime le LIF mgmtlif2 :

```
network interface delete -vserver vs1 -lif mgmtlif2
```

3. Utilisez le `network interface show` Commande pour confirmer que la LIF est supprimée.

Pour en savoir plus, `network interface show` consultez le ["Référence de commande ONTAP"](#).

## Configuration des LIF ONTAP Virtual IP (VIP)

Certains data centers nouvelle génération utilisent des mécanismes réseau de couche 3 (IP) qui nécessitent le basculement des LIF sur les sous-réseaux. ONTAP prend en charge les LIF de données IP virtuelles (VIP) et le protocole de routage associé, BGP (Border Gateway Protocol), afin de répondre aux exigences de basculement de ces

réseaux nouvelle génération.

### Description de la tâche

Une LIF de données VIP est une LIF qui ne fait pas partie d'un sous-réseau et est accessible depuis tous les ports qui hébergent une LIF BGP dans le même IPspace. Une LIF de données VIP élimine la dépendance d'un hôte sur des interfaces réseau individuelles. Étant donné que plusieurs adaptateurs physiques transportent le trafic des données, la charge entière n'est pas concentrée sur un seul adaptateur et le sous-réseau associé. L'existence d'une LIF de données VIP est annoncée pour les routeurs homologues par le biais du protocole de routage, BGP (Border Gateway Protocol).

Les LIF de données VIP offrent les avantages suivants :

- Portabilité de LIF au-delà d'un domaine de broadcast ou d'un sous-réseau : les LIF de données VIP peuvent basculer vers n'importe quel sous-réseau du réseau en annonçant l'emplacement actuel de chaque LIF de données VIP vers des routeurs via BGP.
- Débit global : la LIF de données VIP peut prendre en charge un débit global supérieur à celui d'un port individuel, car les LIF VIP peuvent envoyer ou recevoir simultanément des données provenant de plusieurs sous-réseaux ou ports.

## Configuration du protocole BGP (Border Gateway Protocol)

Avant de créer des LIF VIP, vous devez configurer le protocole BGP, qui est le protocole de routage utilisé pour annoncer l'existence d'une LIF VIP pour les routeurs de l'égal.

À partir de ONTAP 9.9.1, VIP fournit une automatisation de route par défaut facultative à l'aide de groupes de pairs BGP pour simplifier la configuration.

ONTAP offre un moyen simple d'apprendre les routes par défaut en utilisant les pairs BGP comme routeurs de saut suivant lorsque l'homologue BGP se trouve sur le même sous-réseau. Pour utiliser la fonction, définissez l' `-use-peer-as-next-hop` attribut à `true`. Par défaut, cet attribut est `false`.

Si vous avez des routes statiques configurées, celles-ci sont encore préférées sur ces routes automatisées par défaut.

### Avant de commencer

Le routeur homologue doit être configuré pour accepter une connexion BGP à partir du LIF BGP pour le numéro de système autonome configuré (ASN).



ONTAP ne traite aucune annonce de route entrante à partir du routeur ; par conséquent, vous devez configurer le routeur homologue pour qu'il n'envoie aucune mise à jour de route au cluster. Cela réduit le temps nécessaire à la communication avec l'homologue pour devenir entièrement fonctionnel et réduit l'utilisation de la mémoire interne dans ONTAP.

### Description de la tâche

La configuration du protocole BGP implique la création d'une configuration BGP, la création d'une LIF BGP et la création d'un groupe de pairs BGP. ONTAP crée automatiquement une configuration BGP par défaut avec des valeurs par défaut lorsque le premier groupe de pairs BGP est créé sur un nœud donné.

Une LIF BGP est utilisée pour établir des sessions TCP BGP avec des routeurs homologues. Pour un routeur homologue, une LIF BGP est le prochain saut pour atteindre une LIF VIP. Le basculement est désactivé pour le LIF BGP. Un groupe de pairs BGP annonce les routes VIP pour tous les SVM dans l'IPspace utilisé par le groupe de pairs. L'IPspace utilisé par le groupe de pairs est hérité de la LIF BGP.

À partir de ONTAP 9.16.1, l'authentification MD5 est prise en charge sur les groupes de pairs BGP pour protéger les sessions BGP. Lorsque MD5 est activé, les sessions BGP ne peuvent être établies et traitées que parmi les pairs autorisés, ce qui empêche les interruptions potentielles de la session par un acteur non autorisé.

Les champs suivants ont été ajoutés aux `network bgp peer-group create` commandes et `network bgp peer-group modify` :

- `-md5-enabled <true/false>`
- `-md5-secret <md5 secret in string or hex format>`

Ces paramètres vous permettent de configurer un groupe de pairs BGP avec une signature MD5 pour une sécurité renforcée. Les conditions suivantes s'appliquent à l'utilisation de l'authentification MD5 :

- Vous ne pouvez spécifier le paramètre `-md5-secret` lorsque le `-md5-enabled` paramètre est défini sur `true`.
- IPsec doit être activé globalement avant de pouvoir activer l'authentification MD5 BGP. La LIF BGP n'est pas nécessaire pour avoir une configuration IPsec active. Reportez-vous à la "["Configurez la sécurité IP \(IPsec\) sur le cryptage filaire"](#)".
- NetApp vous recommande de configurer MD5 sur le routeur avant de le configurer sur le contrôleur ONTAP.

Depuis ONTAP 9.9.1, ces champs ont été ajoutés :

- `-asn` Ou `-peer-asn` (valeur de 4 octets) l'attribut lui-même n'est pas nouveau, mais il utilise maintenant un entier de 4 octets.
- `-med`
- `-use-peer-as-next-hop`

Vous pouvez effectuer des sélections avancées de route grâce à la prise en charge du décriminateur multi-sortie (MED) pour la hiérarchisation des chemins. MED est un attribut facultatif du message de mise à jour BGP qui indique aux routeurs de sélectionner le meilleur itinéraire pour le trafic. Le MED est un entier 32 bits non signé (0 - 4294967295) ; les valeurs inférieures sont préférées.

Depuis ONTAP 9.8, ces champs ont été ajoutés au `network bgp peer-group` commande :

- `-asn-prepend-type`
- `-asn-prepend-count`
- `-community`

Ces attributs BGP permettent de configurer le EN TANT qu'attributs de chemin et de communauté pour le groupe de pairs BGP.

 Bien que ONTAP prenne en charge les attributs BGP ci-dessus, les routeurs n'ont pas besoin de les honorer. NetApp vous recommande fortement de confirmer les attributs pris en charge par votre routeur et de configurer les groupes de pairs BGP en conséquence. Pour plus de détails, reportez-vous à la documentation BGP fournie par votre routeur.

## Étapes

1. Connectez-vous au niveau de privilège avancé :

```
set -privilege advanced
```

2. Facultatif : créez une configuration BGP ou modifiez la configuration par défaut du cluster en effectuant l'une des opérations suivantes :

a. Créez une configuration BGP :

```
network bgp config create -node {node_name | local} -asn <asn_number>  
-holdtime  
<hold_time> -routerid <router_id>
```



- Le **-routerid** paramètre accepte une valeur de 32 bits à virgule décimale à points qui ne doit être unique que dans un domaine AS. NetApp vous recommande d'utiliser l'adresse IP de gestion des nœuds (v4) <router\_id> pour garantir leur caractère unique.
- Bien que ONTAP BGP prenne en charge les nombres ASN 32 bits, seule la notation décimale standard est prise en charge. La notation ASN en pointillés, telle que 65000.1 au lieu de 4259840001 pour un ASN privé, n'est pas prise en charge.

Échantillon avec un ASN de 2 octets :

```
network bgp config create -node node1 -asn 65502 -holdtime 180  
-routerid 1.1.1.1
```

Exemple avec un ASN de 4 octets :

```
network bgp config create -node node1 -asn 85502 -holdtime 180 -routerid  
1.1.1.1
```

a. Modifiez la configuration BGP par défaut :

```
network bgp defaults modify -asn <asn_number> -holdtime <hold_time>  
network bgp defaults modify -asn 65502 -holdtime 60
```

- <asn\_number> Spécifie le numéro ASN. À partir de ONTAP 9.8, ASN pour BGP prend en charge un entier non négatif de 2 octets. Il s'agit d'un nombre de 16 bits (1 à 65534 valeurs disponibles). À partir de ONTAP 9.9.1, ASN pour BGP prend en charge un entier non négatif de 4 octets (1 à 4294967295). L'ASN par défaut est 65501. ASN 23456 est réservé à l'établissement de session ONTAP avec des pairs qui n'annoncent pas la capacité ASN de 4 octets.
- <hold\_time> spécifie le temps de maintien en secondes. La valeur par défaut est 180s.



ONTAP ne prend en charge qu'un seul global <asn\_number>, <hold\_time>, , et <router\_id>, même si vous configurez BGP pour plusieurs IPspaces. Le BGP et toutes les informations de routage IP sont complètement isolés au sein d'un IPspace. Un IPspace est équivalent à une instance de routage et de transfert virtuel (VRF).

### 3. Créez une LIF BGP pour le SVM du système :

Pour l'IPspace par défaut, le nom du SVM correspond au nom du cluster. Pour les IPspaces supplémentaires, le nom du SVM est identique au nom IPspace.

```
network interface create -vserver <system_svm> -lif <lif_name> -service-policy default-route-announce -home-node <home_node> -home-port <home_port> -address <ip_address> -netmask <netmask>
```

Vous pouvez utiliser le default-route-announce Politique de service pour le LIF BGP ou toute règle de services personnalisée qui contient le service « management-bgp ».

```
network interface create -vserver cluster1 -lif bgp1 -service-policy default-route-announce -home-node cluster1-01 -home-port e0c -address 10.10.10.100 -netmask 255.255.255.0
```

### 4. Créez un groupe d'homologues BGP utilisé pour établir des sessions BGP avec les routeurs homologues distants et configurer les informations de routage VIP annoncées aux routeurs homologues :

Exemple 1 : créez un groupe de pairs sans route par défaut automatique

Dans ce cas, l'administrateur doit créer une route statique vers l'homologue BGP.

```
network bgp peer-group create -peer-group <group_name> -ipspace <ipspace_name> -bgp-lif <bgp_lif> -peer-address <peer-router_ip_address> -peer-asn <peer_asn_number> {-route-preference <integer>} {-asn-prepend-type <ASN-prepend_type>} {-asn-prepend-count <integer>} {-med <integer>} {-community BGP community list <0-65535>:<0-65535>}
```

```
network bgp peer-group create -peer-group group1 -ipspace Default -bgp -lif bgp1 -peer-address 10.10.10.1 -peer-asn 65503 -route-preference 100 -asn-prepend-type local-asn -asn-prepend-count 2 -med 100 -community 9000:900,8000:800
```

Exemple 2 : créez un groupe de pairs avec une route par défaut automatique

```
network bgp peer-group create -peer-group <group_name> -ipspace
<ipspace_name> -bgp-lif <bgp_lif> -peer-address <peer-router_ip_address>
-peer-asn <peer_asn_number> {-use-peer-as-next-hop true} {-route-
preference <integer>} {-asn-prepend-type <ASN_prepend_type>} {-asn-
prepend-count <integer>} {-med <integer>} {-community BGP community list
<0-65535>:<0-65535>}
```

```
network bgp peer-group create -peer-group group1 -ipspace Default -bgp
-lif bgp1 -peer-address 10.10.10.1 -peer-asn 65503 -use-peer-as-next-hop
true -route-preference 100 -asn-prepend-type local-asn -asn-prepend
-count 2 -med 100 -community 9000:900,8000:800
```

Exemple 3 : créez un groupe de pairs avec MD5 activé

a. Activer IPsec :

```
security ipsec config modify -is-enabled true
```

b. Créez le groupe de pairs BGP avec MD5 activé :

```
network bgp peer-group create -ipspace Default -peer-group
<group_name> -bgp-lif bgp_lif -peer-address <peer_router_ip_address>
{-md5-enabled true} {-md5-secret <md5 secret in string or hex format>}
```

Exemple avec une clé hexagonale :

```
network bgp peer-group create -ipspace Default -peer-group peer1 -bgp
-lif bgp_lif1 -peer-address 10.1.1.100 -md5-enabled true -md5-secret
0x7465737420736563726574
```

Exemple d'utilisation d'une chaîne :

```
network bgp peer-group create -ipspace Default -peer-group peer1 -bgp
-lif bgp_lif1 -peer-address 10.1.1.100 -md5-enabled true -md5-secret "test
secret"
```

Après avoir créé le groupe de pairs BGP, un port ethernet virtuel (en commençant par v0a..v0z,v1a...) apparaît lorsque vous exécutez la `network port show` commande. Le MTU de cette interface est toujours indiqué à 1500. Le MTU réel utilisé pour le trafic est dérivé du port physique (BGP LIF), qui est déterminé lors de l'envoi du trafic. Pour en savoir plus, `network port show` consultez le ["Référence de commande ONTAP"](#).



## Créer une LIF de données VIP (Virtual IP)

L'existence d'une LIF de données VIP est annoncée pour les routeurs homologues par le biais du protocole de routage, BGP (Border Gateway Protocol).

### Avant de commencer

- Le groupe de pairs BGP doit être configuré et la session BGP pour le SVM sur lequel la LIF est créée doit être active.
- Une route statique vers le routeur BGP ou tout autre routeur du sous-réseau de la LIF BGP doit être créée pour tout trafic VIP sortant pour la SVM.
- Vous devez activer le routage multivoie afin que le trafic VIP sortant puisse utiliser toutes les routes disponibles.

Si le routage multichemin n'est pas activé, tout le trafic VIP sortant passe à partir d'une interface unique.

### Étapes

#### 1. Créer une LIF de données VIP :

```
network interface create -vserver <svm_name> -lif <lif_name> -role data
-data-protocol
{ nfs|cifs|iscsi|fcache|none|fc-nvme } -home-node <home_node> -address
<ip_address> -is-vip true -failover-policy broadcast-domain-wide
```

Un port VIP est automatiquement sélectionné si vous ne spécifiez pas le port d'accueil avec le `network interface create` commande.

Par défaut, la LIF de données VIP appartient au domaine de diffusion créé par le système, nommé « VIP », pour chaque IPspace. Vous ne pouvez pas modifier le broadcast domain VIP.

Une LIF de données VIP est accessible simultanément sur tous les ports hébergeant une LIF BGP d'un IPspace. En l'absence de session BGP active pour le SVM de VIP sur le nœud local, la LIF de données VIP bascule vers le port VIP suivant sur le nœud sur lequel une session BGP est établie pour ce SVM.

#### 2. Vérifier que la session BGP est au statut up pour le SVM de la LIF de données VIP :

```
network bgp vserver-status show

Node          Vserver  bgp status
-----  -----
node1        vs1      up
```

Si le statut BGP est de `down` Pour le SVM sur un nœud, la LIF de données VIP bascule vers un nœud différent où l'état BGP est activé pour le SVM. Si le statut BGP est de `down` Sur tous les nœuds, la LIF de données VIP ne peut pas être hébergée n'importe où et possède le statut LIF comme étant arrêté.

## Commandes de gestion du protocole BGP

À partir de ONTAP 9.5, vous utilisez le `network bgp` Commandes permettant de gérer les sessions BGP dans ONTAP.

### Gérer la configuration BGP

Les fonctions que vous recherchez...	Utilisez cette commande...
Créez une configuration BGP	<code>network bgp config create</code>
Modifiez la configuration BGP	<code>network bgp config modify</code>
Supprimez la configuration BGP	<code>network bgp config delete</code>
Affiche la configuration BGP	<code>network bgp config show</code>
Affiche l'état BGP pour le SVM de la LIF VIP	<code>network bgp vserver-status show</code>

### Gérer les valeurs par défaut du protocole BGP

Les fonctions que vous recherchez...	Utilisez cette commande...
Modifiez les valeurs par défaut du protocole BGP	<code>network bgp defaults modify</code>
Affiche les valeurs par défaut du protocole BGP	<code>network bgp defaults show</code>

### Gérez les groupes de pairs BGP

Les fonctions que vous recherchez...	Utilisez cette commande...
Créez un groupe de pairs BGP	<code>network bgp peer-group create</code>
Modifiez un groupe de pairs BGP	<code>network bgp peer-group modify</code>
Supprimez un groupe de pairs BGP	<code>network bgp peer-group delete</code>
Affiche les informations sur les groupes de pairs BGP	<code>network bgp peer-group show</code>
Renommez un groupe d'homologues BGP	<code>network bgp peer-group rename</code>

### Gérez les groupes de pairs BGP avec MD5

À partir de ONTAP 9.16.1, vous pouvez activer ou désactiver l'authentification MD5 sur un groupe de pairs BGP existant.



Si vous activez ou désactivez MD5 sur un groupe de pairs BGP existant, la connexion BGP est interrompue et recréée pour appliquer les modifications de configuration MD5.

Les fonctions que vous recherchez...	Utilisez cette commande...
--------------------------------------	----------------------------

Activez MD5 sur un groupe de pairs BGP existant	<pre>network bgp peer-group modify -ipspace Default -peer-group &lt;group_name&gt; -bgp -lif &lt;bgp_lif&gt; -peer-address &lt;peer_router_ip_address&gt; -md5-enabled true -md5-secret &lt;md5 secret in string or hex format&gt;</pre>
Désactivez MD5 sur un groupe de pairs BGP existant	<pre>network bgp peer-group modify -ipspace Default -peer-group &lt;group_name&gt; -bgp -lif &lt;bgp_lif&gt; -md5-enabled false</pre>

#### Informations associées

- ["Référence de commande ONTAP"](#)
- ["bgp réseau"](#)
- ["interface réseau"](#)
- ["modification de la configuration de sécurité IPsec"](#)

## Informations sur le copyright

Copyright © 2026 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUSSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

**LÉGENDE DE RESTRICTION DES DROITS :** L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

## Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.